RECEIVED
CENTRAL FAX CENTER
JUN 0 3 2008

In the Claims

Claims remaining in the application are as follows:

1. (Currently amended): A method for establishing a secure channel through an indeterminate number of nodes in a network comprising:

enrolling a smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the ~~secret~~ unique key;

transacting at a point of entry to the network, the transaction creating a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and transaction sequence number;

communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network; and

recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key.

2. (Original): The method according to Claim 1 further comprising:

defining public key values (e, N) that are exclusive to a card issuer system and card base, the key value e being a public exponent and the key value N being a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system;

defining a private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key;

computing a secret key u that is unique to the smart card using an equation of the form:

$$u = x^d (\mathrm{mod}\ N),$$

where x is an entity-identifier that identifies the smart card and the entity; and storing the secret key u on the smart card with public key values x, e, and N.

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

PAGE 4/19 * RCVD AT 6/3/2008 8:36:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/9 * DNIS:2738300 * CSID:9492510260 * DURATION (mm-ss):05-14

3. (Original): The method according to Claim 1 further comprising:
receiving at an entity-activated terminal an entity-entered Personal Identification Number (PIN) and an entity-inserted smart card;
passing the PIN to the smart card;
computing at the smart card an equation of the form:

$$K = u \cdot TSN^{H} (\mathrm{mod}\ N),$$

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and
hashing at the smart card the keying code K to form the PIN encryption key KPE according to an equation of the form:

$$KPE = h(K),$$

where h() is a hashing algorithm.

4. (Original): The method according to Claim 3 further comprising:
hashing at the smart card the keying code K to form an encryption key according to an encryption definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

5. (Original): The method according to Claim 3 further comprising:
padding the keying code K with transaction-related data prior to the hash operation h(K).

6. (Original): The method according to Claim 3 further comprising:
deriving the PIN encryption key KPE uniquely as a function of the secret key u for each transaction, the encryption key KPE being secure from an adversary because the secret key u is unknown.

KOESTNER BERTANI LLP
2192 MARTIN ST
SUITE 150
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

7. (Currently amended): The method according to Claim 6 further comprising: maintaining the private key value d as a secret known only to the card issuer as the only entity capable of decrypting ~~the cryptogram C~~ a cryptogram C.

8. (Original): The method according to Claim 1 further comprising:
receiving a PIN encryption key KPE at a card issuer server;
computing a hash H of transaction data;
computing an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t of a transaction sequence identifier TSN that identifies a transaction terminal and a sequence number for a transaction originating at the terminal according to an equation of the form:

$$t = TSN^e (\mathrm{mod}\ N),$$

where N is a modulus in an RSA system;
computing a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H (\mathrm{mode}\ N),$$

where x is an entity-identifier that identifies the smart card and the entity;
decrypting the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d (\mathrm{mod}\ N);\ \text{and}$$

decrypting the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

9. (Original): The method according to Claim 1 further comprising:
encrypting a PIN at the smart card using perfect forward secrecy based on a random number generation whereby compromise of persistent secret data does not jeopardize data security of prior transactions.

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

10. (Original): The method according to Claim 1 further comprising:
receiving at an entity-activated terminal an entity-entered Personal Identification Number (PIN) and an entity-inserted smart card;
passing the PIN to the smart card;
generating a random number r at the smart card that is unique to a transaction;
computing at the smart card an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t according to an equation of the form:

$$t = r^e (\text{mod } N),$$

where e is the public exponent and N the modulus of the RSA system;
computing at the smart card a hash H of common public transaction data;
computing at the smart card a keying code K and a PIN encryption key KPE according to equations of the form:

$$K = u \cdot r^H (\text{mod } N), \text{ and}$$

$$KPE = h(K),$$

where u is a secret key and H is a hash of transaction data elements, and
sending the PIN encryption key KPE and RSA system encryption t through the network; and
erasing the random number r.

11. (Original): The method according to Claim 10 further comprising:
receiving a PIN encryption key KPE and encryption t at a card issuer server;
computing a hash H of transaction data;
computing a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H (\text{mode } N),$$

where x is an entity-identifier that identifies the smart card and the entity;
decrypting the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d (\text{mod } N); \text{ and}$$

KOESTNER BERTANI LLP
2192 MARTIN ST. SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

decrypting the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

12. (Original): The method according to Claim 1 further comprising:
computing at the smart card a hash H of transaction data;
communicating the transaction data hash to a card issuer server;
computing at the card issuer server a hash of transaction data; and
verifying the communicated hash with the server-computed hash for authentication and integrity checking.

13. (Currently amended): A data security apparatus comprising:
a smart card ~~capable of establishing~~ that establishes a secure channel through an indeterminate number of nodes in a network comprising:
an interface ~~capable of~~ for communicating with a card reader and/or writer;
a processor coupled to the interface; ~~and~~
a memory coupled to the processor that stores a public entity-identifier and a secret unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, the memory further comprising:
a computable readable program code embodied therein that creates a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies ~~the point~~ a point of entry and transaction sequence number;
a computable readable program code ~~capable of~~ causing the processor to receive an entity-entered Personal Identification Number (PIN);
a computable readable program code causing the processor to compute an equation of the form:

$$K = u \cdot TSN^{H} (\text{mod } N),$$

KOESTNER BERTANI LLP
3192 MARTIN ST
SUITE 150
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and

a computable readable program code causing the processor to hash the keying code K to form the PIN encryption key KPE according to an equation of the form:

$$KPE = h(K),$$

where h() is a hashing algorithm.

14. (Original): The apparatus according to Claim 13 further comprising:

a secret unique key u stored in the memory with public key values x, e, and N where x is an entity-identifier that identifies the smart card and the entity, a key value e is a public exponent and a key value N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system, the public key values (e, N) being exclusive to a card issuer system and card base; wherein:

the secret key u is unique to the smart card and computed using an equation of the form:

$$u = x^d (\text{mod } N),$$

where a private key value d is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key.

15. (Canceled).

16. (Currently amended): The apparatus according to ~~Claim 15~~ Claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash the keying code K to form an encryption key according to an encryption

KOESTNER BERTANI LLP
3191 MARTIN ST
SUITE 150
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

17. (Currently amended): The apparatus according to ~~Claim 15~~ Claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to pad the keying code K with transaction-related data prior to the hash operation h(K).

18. (Canceled).

19. (Currently amended): The apparatus according to Claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash transaction data elements and communicate the hash point-to-point to a card issuer enabling simultaneous key management and integrity checking.

20. (Currently amended): A data security apparatus comprising:

an enrollment system ~~capable of usage for establishing~~ that establishes a secure channel through an indeterminate number of nodes in a network, the enrollment system comprising:

a communication interface ~~capable of~~ for communicating with a writer configured to accept a smart card;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein ~~capable of~~ causing the processor to initialize and personalize ~~a smart~~ the smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, the unique key for usage by the smart card to create a PIN encryption key computed by an equation of the form:

KOESTNER BERTANI LLP
3193 MARTIN ST.
SUITE 150
IRVINE, CA 92613
TEL (949) 251-0250
FAX (949) 251-0260

$K = u \cdot TSN^H (\mathrm{mod}\ N)$,

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and

the smart card hashes the keying code K to form the PIN encryption key KPE according to an equation of the form:

$KPE = h(K)$,

where h() is a hashing algorithm.

21. (Currently amended): The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to write to an enrolled smart card a stored public entity-identifier and the secret unique key.

22. (Currently amended): The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to define public key values (e, N) that are exclusive to a card issuer system and card base, the key value e being a public exponent and the key value N being a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system;

a computable readable program code ~~capable of~~ causing the processor to define a private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key;

a computable readable program code ~~capable of~~ causing the processor to compute a secret key u that is unique to the smart card using an equation of the form:

KOESTNER BERTANI LLP
2192 MARTIN ST, SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0360

$u = x^d (\mathrm{mod}\ N)$,

where x is an entity-identifier that identifies the smart card and the entity; and

a computable readable program code ~~capable of~~ causing the processor to store the secret key u on the smart card with public key values x, e, and N.

23. (Currently amended): A data security apparatus comprising:

a card issuer server ~~capable of usage for establishing~~ <u>that establishes</u> a secure channel through an indeterminate number of nodes in a network, the card issuer server comprising:

a communication interface ~~capable of~~ <u>for</u> communicating with the network;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein ~~capable of~~ causing the processor to recover a Personal Identification Number (PIN) from a transaction PIN encryption key received via the network using a card issuer private key, the transaction PIN encryption key being derived from a smart card unique key initialized and personalized to the smart card and derived from the card issuer private key, and a transaction identifier that uniquely identifies the point of entry and <u>a</u> transaction sequence number.

24. (Original): The apparatus according to Claim 23 wherein:

the smart card unique key is a secret key u that is unique to the smart card and is computed by a card enrollment system using an equation of the form:

$u = x^d (\mathrm{mod}\ N)$,

where x is an entity-identifier that identifies the smart card and the entity; a private key value d is a secret RSA private key, and key value N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

Cryptosystem) system, the key values d and N being exclusive to a card issuer system and card base.

25. (Currently amended): The apparatus according to Claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to receive a PIN encryption key KPE at a card enrollment server;

a computable readable program code ~~capable of~~ causing the processor to compute a hash H of transaction data;

a computable readable program code ~~capable of~~ causing the processor to compute an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t of a transaction sequence identifier TSN that identifies a transaction terminal and a sequence number for a transaction originating at the terminal according to an equation of the form:

$$t = TSN^e (\mathrm{mod}\ N),$$

where N is a modulus in an RSA system;

a computable readable program code ~~capable of~~ causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H (\mathrm{mode}\ N),$$

where x is an entity-identifier that identifies the smart card and the entity;

a computable readable program code ~~capable of~~ causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d (\mathrm{mod}\ N);\ \text{and}$$

a computable readable program code ~~capable of~~ causing the processor to decrypt the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

26. (Currently amended): The apparatus according to Claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to receive a PIN encryption key KPE and encryption t;

a computable readable program code ~~capable of~~ causing the processor to compute a hash H of transaction data;

a computable readable program code ~~capable of~~ causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$$C = x \cdot t^H (\text{mode } N),$$

where x is an entity-identifier that identifies the smart card and the entity;

a computable readable program code ~~capable of~~ causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K = C^d (\text{mod } N); \text{ and}$$

a computable readable program code ~~capable of~~ causing the processor to decrypt the PIN using the PIN encryption key KPE = h(K) where h() is a hashing algorithm.

27. (Currently amended): The apparatus according to Claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash transaction data elements and compare the hash from a hash received point-to-point from a smart card enabling simultaneous key management and integrity checking.

KOESTNER BERTANI LLP
2192 MARTIN ST
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

28. (Currently amended): A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupling to the network;

a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;

a plurality of smart cards enrolled in the transaction system and capable of insertion into the terminals and transacting via the servers; and

a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors ~~being capable of~~ establishing a secure channel through an indeterminate number of nodes in the network by creating, communicating, and decrypting a PIN encryption key derived from a smart card unique key and a transaction identifier that uniquely identifies a point of entry terminal and transaction sequence number, the smart card unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer.

29. (Currently amended): A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupling to the network;

a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;

a plurality of smart cards enrolled in the transaction system and capable of insertion into the terminals and transacting via the servers; and

a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors ~~being capable of~~ establishing a secure channel through an indeterminate number of nodes in the network by creating, communicating, and decrypting a PIN encryption key derived from a smart card unique key and a hash of transaction data elements, enabling simultaneous key management and integrity checking.

KOESTNER BERTANI LLP
2192 MARTIN ST
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

30. (Currently amended): A transaction system ~~capable of~~ establishing a secure channel through an indeterminate number of nodes in a network comprising:

means for enrolling a smart card with a unique key per smart card, the unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the secret unique key;

means for transacting at a point of entry to the network, the transaction creating a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and transaction sequence number;

means for communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network; and

means for recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key.

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260